Détection des menaces spécifiques

Les rubriques suivantes expliquent comment utiliser des préprocesseurs dans une politique d'analyse de réseau pour détecter des menaces spécifiques :

Introduction à la détection de menaces spécifiques

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous pouvez utiliser plusieurs préprocesseurs dans une politique d'analyse de réseau pour détecter des menaces spécifiques pour votre réseau surveillé, telles que les attaques back Orifice (par ouverture arrière), plusieurs types de balayage de ports et les attaques basées sur le débit qui tentent de submerger votre réseau avec un trafic excessif. Lorsque les signatures GID spécifiques au préprocesseur sont activées, la politique d'analyse de réseau sur le Web affichera Désactivée. Cependant, les préprocesseurs seront activés sur le périphérique en utilisant les paramètres par défaut disponibles.

Vous pouvez également utiliser la détection des données sensibles, que vous configurez dans une politique de prévention des intrusions, pour détecter la transmission non sécurisée de données numériques sensibles.

Licences requises pour la détection de menaces spécifiques

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables requises pour la détection de menaces spécifiques

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Détection Back Orifice (ouverture arrière)

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le système Firepower fournit un préprocesseur qui détecte l'existence du programme Back Orifice. Ce programme peut être utilisé pour obtenir un accès administrateur à vos hôtes Windows.

Préprocesseur de détection de l'ouverture arrière

Le préprocesseur de l'ouverture arrière analyse le trafic UDP à la recherche du témoin magique de l'ouverture arrière, « `!*QWTY?` », qui se trouve dans les huit premiers octets du paquet et qui est chiffré par XOR.

Le préprocesseur de l'ouverture arrière comporte une page de configuration, mais aucune option de configuration. Lorsqu'il est activé, vous devez également activer les règles de préprocesseur pour le préprocesseur générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 1 : Ouverture arrière GID : SID

GID de règle de préprocesseur : SID	Description
105:1	Trafic de l'ouverture arrière détecté

GID de règle de préprocesseur : SID	Description
105:2	Trafic client de l'ouverture arrière détecté
105:3	Trafic serveur de l'ouverture arrière détecté
105:4	Attaque de la mémoire tampon Snort de l'ouverture arrière détectée

Détection de l'ouverture arrière

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si la **détection de l'ouverture arrière** sous **Détection des menaces spécifiques** est désactivée, cliquez sur **Activée**.

Remarque Il n'y a pas d'options configurables par l'utilisateur pour la fonction Back Orifice.

Étape 6 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de détection de l'iris retour 105:1, 105:2, 105:3 ou 105:4. Pour plus de renseignements, consultez les sections États des règles d'intrusion et Préprocesseur de détection de l'ouverture arrière, à la page 2.
- Déployer les changements de configuration.

Détection de balayage de ports

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Un balayage de ports est une forme de reconnaissance du réseau souvent utilisée par les attaquants comme préambule d'une attaque. Lors d'un balayage de ports, un attaquant envoie des paquets spécialement conçus à un hôte ciblé. En examinant les paquets avec lesquels l'hôte répond, l'attaquant peut souvent déterminer quels ports sont ouverts sur l'hôte et, soit directement, soit par inférence, quels protocoles d'application sont exécutés sur ces ports.

En soi, un balayage de ports n'est pas une preuve d'une attaque. En fait, certaines des techniques de balayage de ports utilisées par les agresseurs peuvent également être employées par des utilisateurs légitimes de votre réseau. Le détecteur d'analyses de ports de Cisco est conçu pour vous aider à déterminer quels balayages de ports pourraient être malveillants en détectant les schémas d'activité.

Attention L'inspection d'équilibre de charge des périphériques entre les ressources internes. Si la détection de balayage de ports ne fonctionne pas comme prévu, vous devrez peut-être configurer le niveau de sensibilité comme **Élevé**.

Nous vous recommandons fortement d'effectuer une mise à niveau vers Snort 3 et d'utiliser la fonction de balayage de ports introduite dans la version 7.2.0. Pour en savoir plus, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 et Référence de l'inspecteur Snort 3.

Types de balayage de ports, protocoles et niveaux de sensibilité des filtres

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les attaquants sont susceptibles d'utiliser plusieurs méthodes pour sonder votre réseau. Souvent, ils utilisent des protocoles différents pour obtenir des réponses différentes d'un hôte cible, en attendant que si un type de protocole est bloqué, un autre soit disponible.

Tableau 2 : Types de protocole

Protocole	Description
TCP	Détecte les sondes TCP telles que les analyses SYN, les analyses ACK, les analyses TCP connect() et les analyses avec des combinaisons d'indicateurs inhabituelles telles que Xmas tree, FIN et NULL
UDP	Détecte les sondes UDP telles que les paquets UDP de zéro octet
ICMP	Détecte les demandes ECHO ICMP (pings)
IP	Détecte les analyses de protocole IP. Ces analyses sont différentes des analyses TCP et UDP, car l'attaquant, au lieu de chercher des ports ouverts, essaie de découvrir quels protocoles IP sont pris en charge sur un hôte cible.

Les balayages de ports sont généralement divisés en quatre types en fonction du nombre d'hôtes ciblés, du nombre d'hôtes à analyser et du nombre de ports qui sont analysés.

Tableau 3 : Types de balayage de ports

Type	Description
Détection de balayage de ports	Une analyse de ports un à un dans laquelle un attaquant utilise un ou plusieurs hôtes pour analyser plusieurs ports sur un seul hôte cible. Les balayages de ports un à un se distinguent par les éléments suivants : • un nombre réduit d'hôtes d'analyse • un hôte unique qui est analysé • un nombre élevé de ports analysés Cette option détecte les balayages de ports TCP, UDP et IP.
Balayage de ports multiples	Un balayage de ports un vers plusieurs dans lequel un attaquant utilise un ou plusieurs hôtes pour analyser un seul port sur plusieurs hôtes cibles. Les balayages de ports se caractérisent par : • un nombre réduit d'hôtes d'analyse • un nombre élevé d'hôtes analysés • un faible nombre de ports uniques analysés Cette option détecte les balayages de ports TCP, UDP, ICMP et IP.

Type	Description
Balayage de ports de leurre	Une analyse de ports un à un dans laquelle l'agresseur associe de fausses adresses IP sources à l'adresse IP d'analyse réelle. Les balayages de ports de leurre se caractérisent par : • un nombre élevé d'hôtes d'analyse • un faible nombre de ports qui ne sont analysés qu'une seule fois • un seul hôte analysé (ou un faible nombre) L'option de balayage de ports de leurre détecte les balayages de ports des protocoles TCP, UDP et IP.
Balayage de ports distribués	Un balayage de ports plusieurs-à-un dans lequel plusieurs hôtes interrogent un seul hôte pour connaître les ports ouverts. Les balayages de ports distribués se caractérisent par : • un nombre élevé d'hôtes d'analyse • un nombre élevé de ports qui ne sont analysés qu'une seule fois • un seul hôte analysé (ou un faible nombre) L'option de balayage distribué des ports détecte les balayages des ports des protocoles TCP, UDP et IP.

Les informations que le détecteur de balayage de ports reçoit à propos d'une sonde sont en grande partie basées sur l'observation de réponses négatives des hôtes sondés. Par exemple, lorsqu'un client Web tente de se connecter à un serveur Web, il utilise le port 80/tcp et on peut compter sur le serveur pour avoir ce port ouvert. Cependant, lorsqu'un agresseur sonde un serveur, il ne sait pas à l'avance s'il offre des services Web. Lorsque le détecteur d'analyse de ports voit une réponse négative (c'est-à-dire un paquet ICMP inaccessible ou un paquet TCP RST), il enregistre la réponse comme une analyse de ports potentielle. Le processus est plus difficile lorsque l'hôte ciblé se trouve de l'autre côté d'un périphérique tel qu'un pare-feu ou un routeur qui filtre les réponses négatives. Dans ce cas, le détecteur de balayage de ports peut générer des événements de balayage de ports *filtrés* en fonction du niveau de sensibilité que vous sélectionnez.

Tableau 4 : Niveaux de sensibilité

Niveau	Description
Faible	Détecte uniquement les réponses négatives des hôtes ciblés. Sélectionnez ce niveau de sensibilité pour supprimer les faux positifs, mais gardez à l'esprit que certains types d'analyses de ports (analyses lentes, analyses filtrées) peuvent être absents. Ce niveau utilise la fenêtre temporelle la plus courte pour la détection du balayage de ports.

Niveau	Description
Moyen	Détecte les balayages de ports en fonction du nombre de connexions à un hôte, ce qui signifie que vous pouvez détecter les balayages de ports filtrés. Cependant, des hôtes très actifs tels que les traducteurs d'adresses réseau et les mandataires peuvent générer des faux positifs. Notez que vous pouvez ajouter les adresses IP de ces hôtes actifs au champ **Ignore scanned** (Ignorer le balayage) pour atténuer ce type de faux positifs. Ce niveau utilise un intervalle temporel plus long pour la détection par balayage de ports.
Élevé	Détecte les balayages de ports en fonction d'une fenêtre temporelle, ce qui signifie que vous pouvez détecter les balayages de ports basés sur le temps. Toutefois, si vous utilisez cette option, vous devez veiller à régler le détecteur au fil du temps en spécifiant les adresses IP dans les champs **Ignore Scanned** (Ignorer le balayage) et **Ignore Scanner** (Ignorer l'analyseur). Ce niveau utilise une fenêtre temporelle beaucoup plus longue pour la détection par balayage de ports.

Génération d'événements par balayage de ports

Lorsque la détection par balayage de ports est activée, vous devez activer les règles avec un ID de générateur (GID) de 122 et un ID de Snort (SID) parmi les SID 1 à 27 pour détecter les différents balayages de ports et balayages de ports.

Remarque Pour les événements générés par le détecteur de connexion de balayage de ports, le numéro de protocole est 255. Étant donné que le balayage de ports n'est pas associé à un protocole particulier par défaut, aucun numéro de protocole n'est attribué à l'interface Internet Attribuée Numbers Authority (IANA). L'IANA désigne 255 comme un numéro réservé, de sorte que ce numéro est utilisé dans les événements d'analyse des ports pour indiquer qu'il n'y a pas de protocole associé à l'événement.

Tableau 5 : SID de détection par balayage de ports (GID 122)

Type de balayage de ports	Protocole	Niveau de sensibilité	SID de règle de préprocesseur
Détection de balayage de ports	TCP	Faible	1
	UDP	De moyen à élevé	5
	ICMP	Faible	17
	IP	De moyen à élevé	21
		Faible	Ne génère pas d'événements.
		De moyen à élevé	Ne génère pas d'événements.
		Faible	9
		De moyen à élevé	13

Type de balayage de ports	Protocole	Niveau de sensibilité	SID de règle de préprocesseur
Balayage de ports multiples	TCP	Faible	3, 27
	UDP	De moyen à élevé	7
	ICMP	Faible	19
	IP	De moyen à élevé	23
		Faible	25
		De moyen à élevé	26
		Faible	11
		De moyen à élevé	15
Balayage de ports de leurre	TCP	Faible	2
	UDP	De moyen à élevé	6
	ICMP	Faible	18
	IP	De moyen à élevé	22
		Faible	Ne génère pas d'événements.
		De moyen à élevé	Ne génère pas d'événements.
		Faible	10
		De moyen à élevé	14
Balayage de ports distribués	TCP	Faible	4
	UDP	De moyen à élevé	8
	ICMP	Faible	20
	IP	De moyen à élevé	24
		Faible	Ne génère pas d'événements.
		De moyen à élevé	Ne génère pas d'événements.
		Faible	12
		De moyen à élevé	16

Affichage des paquets d'événements du balayage de ports

Lorsque vous activez les règles de préprocesseur associées, le détecteur de balayage de ports génère des incidents d'intrusion que vous pouvez afficher comme vous le feriez avec tout autre incident d'intrusion. Cependant, les renseignements présentés dans la vue de paquets sont différents des autres types d'incidents d'intrusion.

Commencez par utiliser les vues d'incidents d'intrusion pour accéder à la vue des paquets pour un événement d'analyse de ports. Notez que vous ne pouvez pas télécharger un paquet d'analyse de ports, car les événements

d'analyse de port uniques sont basés sur plusieurs paquets. cependant, la vue de paquets de l'analyse de ports fournit toutes les informations utilisables sur les paquets.

Pour n'importe quelle adresse IP, vous pouvez cliquer dessus pour afficher le menu contextuel et sélectionner **whois** pour effectuer une recherche de l'adresse IP ou **View Host Profile** (afficher le profil d'hôte) pour afficher le profil d'hôte de cet hôte.

Tableau 6 : Vue de paquet du balayage de ports

Information	Description
Périphérique	Le périphérique qui a détecté l'événement
Durée	Heure à laquelle l'événement s'est produit.
Message	Le message d'événement généré par le préprocesseur.
IP de la source	Adresse IP de l'hôte de l'analyse.
IP de la destination	L'adresse IP de l'hôte analysé.
Valeur de la priorité	Le nombre de réponses négatives (par exemple, TCP RST et ICMP unreachables) de la part de l'hôte analysé. Plus le nombre de réponses négatives est élevé, plus la valeur de la priorité est élevé.
Nombre de connexions	Nombre de connexions actives sur les hôtes. Cette valeur est plus précise pour les analyses basées sur la connexion comme TCP et IP.
Nombre d'IP	Le nombre de fois que les adresses IP qui communiquent avec l'hôte analysé changent. Par exemple, si la première adresse IP est 10.1.1.1, la deuxième adresse IP est 10.1.1.2 et la troisième adresse IP est 10.1.1.1, le nombre d'IP est égal à 3. Ce nombre est moins précis pour les hôtes actifs tels que les mandataires et les serveurs DNS.
Plage d'adresses IP analysées/de l'analyseur	La plage d'adresses IP pour les hôtes analysés ou les hôtes de l'analyseur, selon le type d'analyse. Pour le balayage de ports, ce champ affiche la plage d'adresses IP des hôtes analysés. Pour les analyses de ports, ceci indique la plage d'adresses IP des hôtes de l'analyse.
Nombre de ports/protocole	Pour les analyses de ports TCP et UDP, le nombre de fois que le port analysé change. Par exemple, si la valeur du premier port analysé est 80, le deuxième port analysé est le 8080 et le troisième port analysé est à nouveau 80, le nombre de ports est 3. Pour les balayages de ports de protocole IP, le nombre de fois que le protocole utilisé pour se connecter à l'hôte analysé change.
Plage de ports/protocole	Pour les analyses de ports TCP et UDP, la plage des ports qui ont été analysés. Pour les balayages de ports de protocole IP, plage de numéros de protocole IP qui ont été utilisées pour tenter de se connecter à l'hôte analysé.
Ports ouverts	Les ports TCP qui étaient ouverts sur l'hôte analysé. Ce champ s'affiche uniquement lorsque l'analyse de ports détecte un ou plusieurs ports ouverts.

Configuration de la détection de balayage de ports

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les options de configuration de la détection par balayage de ports vous permettent de régler avec précision la façon dont le détecteur de balayage de ports signale l'activité d'analyse.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (Paramètres).

Étape 5 Si **la détection de balayage de ports** sous la **détection de menaces spécifiques** est désactivée, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Détection de balayage de ports**.

Étape 7 Dans le champ **Protocol** (protocole), précisez les protocoles à activer.

Remarque Vous devez vous assurer que le traitement du flux TCP est activé pour détecter les analyses sur TCP et que le traitement du flux UDP est activé pour détecter les analyses sur UDP.

Étape 8 Dans le champ **Scan Type**, précisez les types de balayage de ports que vous souhaitez détecter.

Étape 9 Choisissez un niveau dans la liste **Sensitivity Level** (niveau de sensibilité); voir Types de balayage de ports, protocoles et niveaux de sensibilité des filtres, à la page 4.

Étape 10 Si vous souhaitez surveiller des hôtes spécifiques à la recherche de signes d'activité d'analyse de ports, saisissez l'adresse IP de l'hôte dans le champ **IP de surveillance**.

Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses, ou une liste séparée par des virgules de l'un ou des deux, ou les deux. Laissez ce champ vide pour surveiller tout le trafic réseau.

Étape 11 Si vous souhaitez ignorer les hôtes en tant qu'analyseurs, saisissez l'adresse IP de l'hôte dans le champ **Ignore Scanners** (Ignorer les analyseurs).

Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses, ou une liste séparée par des virgules de l'un ou des deux, ou les deux.

Étape 12 Si vous souhaitez ignorer les hôtes comme cibles d'une analyse, saisissez l'adresse IP de l'hôte dans le champ **Ignore Scanner** (Ignorer l'analyse).

Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses, ou une liste séparée par des virgules de l'un ou des deux, ou les deux.

Astuces Utilisez les champs **Ignore Scanners** et **Ignore Scanned** (Ignorer les analysés))pour indiquer les hôtes de votre réseau qui sont particulièrement actifs. Vous devrez peut-être modifier cette liste d'hôtes au fil du temps.

Étape 13 Si vous souhaitez interrompre la surveillance des sessions captées à mi-chemin, décochez la case **Detect Ack Analyses**.

Remarque La détection des sessions à mi-parcours permet d'identifier les analyses des accusés de réception, mais peut provoquer de faux événements, en particulier sur les réseaux à trafic élevé et où des paquets sont abandonnés.

Étape 14 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez que la détection du balayage de ports détecte diverses analyses de ports et balayages de ports, activez les règles 122:1 à 122:27. Pour plus de renseignements, consultez les sections États des règles d'intrusion et Génération d'événements par balayage de ports, à la page 7.
- Déployer les changements de configuration.

Prévention des attaques basées sur le débit

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les attaques basées sur le débit sont des attaques qui dépendent de la fréquence de connexion ou de tentatives répétées pour perpétrer l'attaque. Vous pouvez utiliser des critères de détection basés sur le débit pour détecter une attaque basée sur le débit dès qu'elle se produit et y intervenir lorsqu'elle se produit, puis revenir aux paramètres de détection normaux après son arrêt.

Vous pouvez configurer votre politique d'analyse de réseau pour inclure des filtres basés sur le débit qui détectent toute activité excessive dirigée contre les hôtes de votre réseau. Vous pouvez utiliser cette fonctionnalité sur les périphériques gérés déployés en mode en ligne pour bloquer les attaques basées sur le

débit pendant une durée spécifiée, puis revenir à la génération uniquement d'événements sans abandonner le trafic.

L'option de prévention des attaques SYN vous aide à protéger vos hôtes réseau contre les inondations SYN. Vous pouvez protéger des hôtes individuels ou des réseaux entiers en fonction du nombre de paquets vus sur une période de temps donnée. Si votre périphérique est déployé de manière passive, vous pouvez générer des événements. Si votre périphérique est placé en ligne, vous pouvez également supprimer les paquets malveillants. Après l'expiration du délai d'expiration, si la condition de débit s'est arrêtée, la génération d'événements et la suppression de paquets s'arrêtent.

Par exemple, vous pouvez configurer un paramètre pour autoriser un nombre maximal de paquets SYN à partir d'une adresse IP et bloquer toute autre connexion à partir de cette adresse IP pendant 60 secondes.

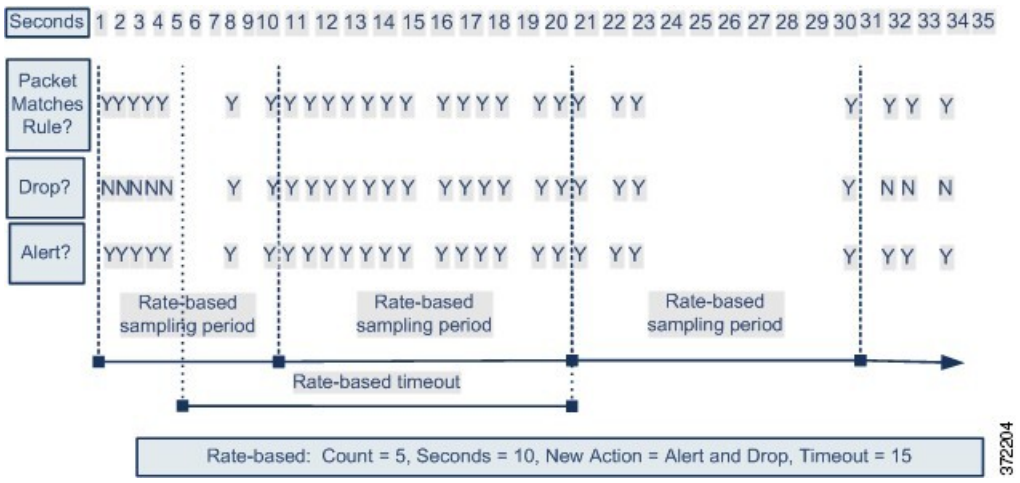
Vous pouvez également limiter les connexions TCP/IP vers ou à partir des hôtes de votre réseau pour éviter les attaques par déni de service ou les activités excessives des utilisateurs. Lorsque le système détecte le nombre configuré de connexions réussies vers ou à partir d'une adresse IP ou d'une plage d'adresses spécifiées, il génère des événements sur des connexions supplémentaires. La génération d'événement basée sur le débit se poursuit jusqu'à ce que le délai d'expiration se soit écoulé sans que la condition de débit ne se produise. Dans un déploiement en ligne, vous pouvez choisir d'abandonner les paquets jusqu'à ce que la condition de débit expire.

Par exemple, vous pouvez configurer un paramètre pour autoriser un maximum de 10 connexions simultanées réussies à partir d'une adresse IP et bloquer toutes les autres connexions à partir de cette adresse IP pendant 60 secondes.

Remarque L'inspection d'équilibre de charge des périphériques entre les ressources internes. Lorsque vous configurez la prévention des attaques basée sur le débit, vous configurez le débit de déclenchement par ressource, et non par périphérique. Si la prévention des attaques basée sur le débit ne fonctionne pas comme prévu, vous devrez peut-être réduire le débit de déclenchement. Il déclenche une alerte si les utilisateurs envoient trop de tentatives de connexion dans des intervalles de temps prescrits. Par conséquent, il est recommandé de limiter le débit à la règle. Pour obtenir de l'aide sur la détermination du débit approprié, communiquez avec le service d'assistance.

Le diagramme suivant montre un exemple dans lequel un agresseur tente d'accéder à un hôte. Les tentatives répétées pour trouver un mot de passe déclenchent une règle pour laquelle la prévention des attaques basée sur le débit est configurée. Les paramètres basés sur le débit remplacent l'attribut de règle par Abandon et génération d'événements après cinq correspondances de règles en 10 secondes. Le nouvel attribut de règle expire après 15 secondes.

Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Si le débit échantillonné est supérieur au seuil au cours de la période d'échantillonnage en cours ou précédente, la nouvelle action se poursuit. La nouvelle action ne revient à la génération d'événements qu'après une période d'échantillonnage pendant laquelle la fréquence échantillonnée est inférieure à la fréquence seuil.



Sujets connexes

États des règles d’intrusion dynamique

Exemples de prévention des attaques basées sur le débit

Le mot-clé `detection_filter` et les fonctionnalités de seuil et de suppression offrent d’autres moyens de filtrer le trafic lui-même ou les événements générés par le système. Vous pouvez utiliser la prévention des attaques basée sur le débit seule ou en combinaison avec un seuil, la suppression ou le mot-clé `detection_filter`.

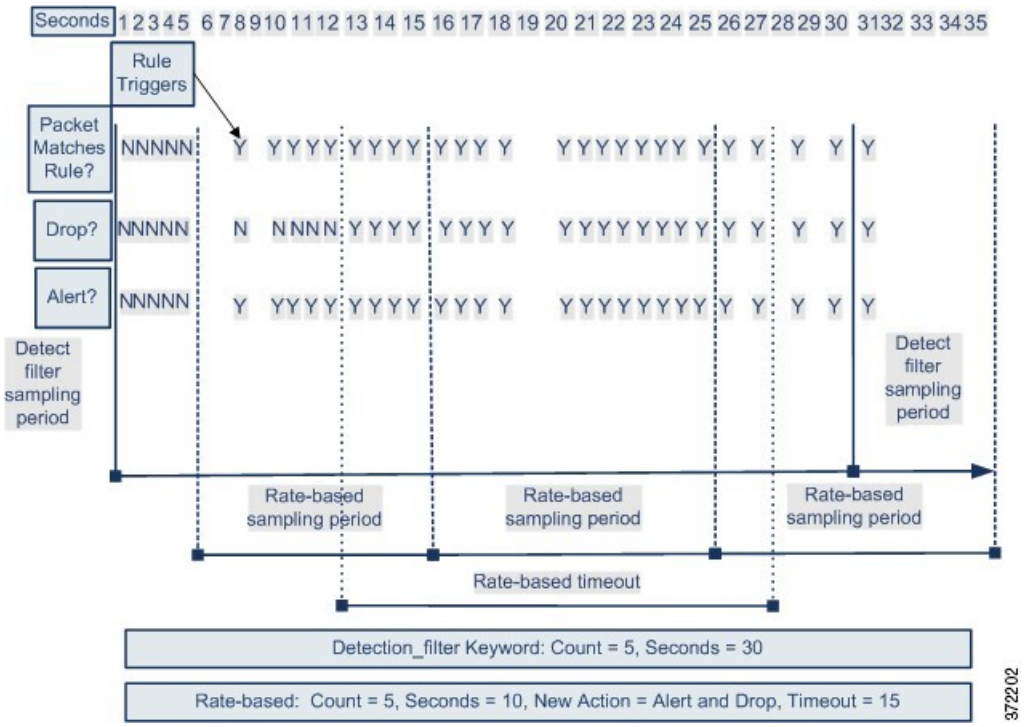
Le mot-clé `detection_filter`, le seuil ou la suppression et les critères basés sur le débit peuvent tous s’appliquer au même trafic. Lorsque vous activez la suppression à une règle, les événements sont supprimés pour les adresses IP précisées même si une modification basée sur le débit se produit.

Exemple de mot-clé detection_filter

L'exemple suivant montre un agresseur tentant une connexion par force brute. Les tentatives répétées pour trouver un mot de passe déclenchent une règle qui inclut également le mot-clé `detection_filter`, avec un nombre défini à 5. Cette règle a configuré la prévention des attaques basée sur le débit. Les paramètres basés sur le débit remplacent l’attribut de règle par Abandon, et génère des événements pendant 20 secondes lorsque la règle compte cinq résultats en 10 secondes.

Comme le montre le diagramme, les cinq premiers paquets correspondant à la règle ne génèrent pas d’événements, car la règle ne se déclenche pas tant que le débit ne dépasse pas le débit indiqué par le mot-clé `detection_filter`. Une fois la règle déclenchée, la notification d’événement commence, mais les critères basés sur le débit ne déclenchent la nouvelle action Abandon and Generate Events que lorsque cinq autres paquets se passent.

Une fois les critères basés sur le débit remplis, des événements sont générés et les paquets sont abandonnés jusqu’à ce que le délai basé sur le débit expire et que le débit tombe sous le seuil. Après vingt secondes, l’action basée sur le débit expire. Après l’expiration du délai, notez que les paquets sont toujours abandonnés durant la période d’échantillonnage basée sur le débit, qui suit. Comme la fréquence échantillonnée est supérieure à la fréquence seuil de la période d’échantillonnage précédente au moment de l’expiration du délai, l’action basée sur la fréquence se poursuit.



Notez que bien que l'exemple ne décrive pas cela, vous pouvez utiliser l'état de règle Abandon et génération d'événements en combinaison avec le mot-clé `detection_filter` pour commencer à abandonner le trafic lorsque les résultats de la règle atteignent le débit spécifié. Avant de décider de configurer les paramètres basés sur le débit pour une règle, déterminez si la définition de la règle comme Abandon et génération d'événements et intégration du mot-clé `detection_filter` produira le même résultat ou si vous souhaitez gérer les paramètres de débit et de délai d'expiration dans la politique de prévention des intrusions.

Sujets connexes

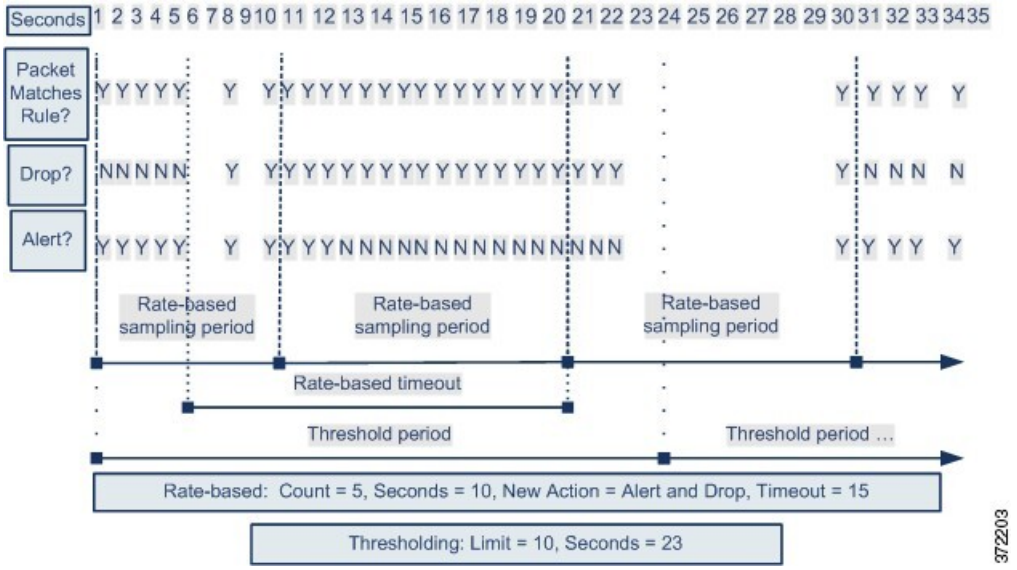
États des règles d'intrusion

Exemple de seuil ou de suppression d'état de règle dynamique

L'exemple suivant montre un agresseur tentant une connexion par force brute. Les tentatives répétées pour trouver un mot de passe déclenchent une règle pour laquelle la prévention des attaques basée sur le débit est configurée. Les paramètres basés sur le débit remplacent l'attribut de règle par Abandon, et génère des événements pendant 15 secondes lorsque la règle compte cinq résultats en 10 secondes. En outre, un seuil de limite limite le nombre d'événements qu'une règle peut générer à 10 en 23 secondes.

Comme l'illustre le diagramme, la règle génère des événements pour les cinq premiers paquets correspondants. Après cinq paquets, les critères basés sur le débit déclenchent la nouvelle action d'abandon et de génération d'événements. Pour les cinq paquets suivants, la règle génère des événements et le système abandonne le paquet. Après le dixième paquet, le seuil limite est atteint. Par conséquent, pour les paquets restants, le système ne génère pas d'événements, mais abandonne les paquets.

Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Si la fréquence échantillonnée est supérieure à la fréquence seuil au cours de la période d'échantillonnage en cours ou précédente, la nouvelle action se poursuit. La nouvelle action ne revient à Générer des événements qu'à la fin d'une période d'échantillonnage pendant laquelle la fréquence échantillonnée est inférieure à la fréquence seuil.



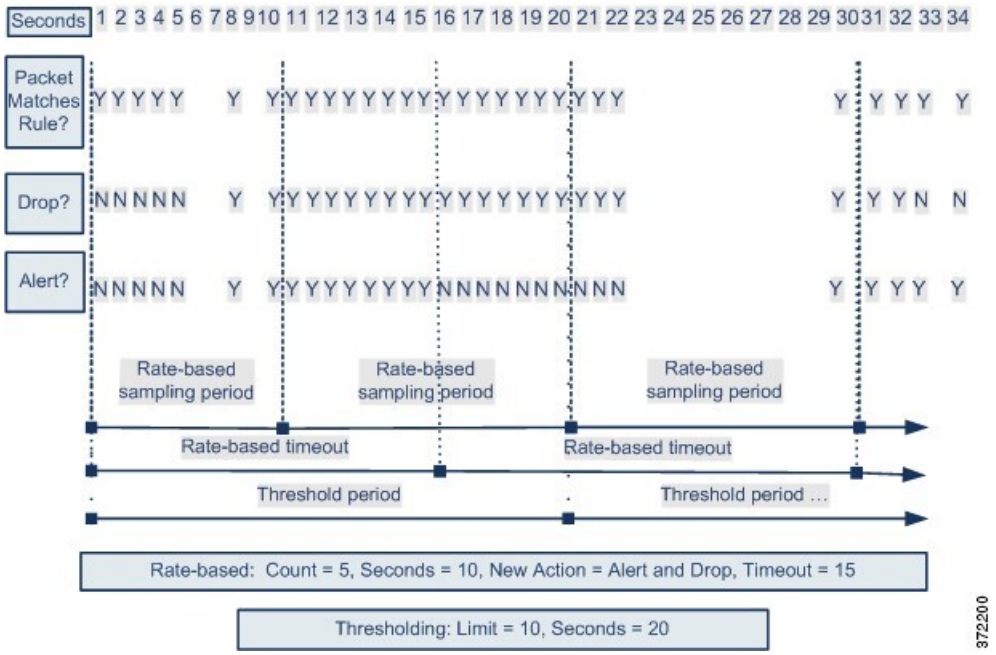
Notez que bien que cela ne soit pas illustré dans cet exemple, si une nouvelle action se déclenche en raison de critères basés sur le débit *après* l'atteinte d'un seuil, le système génère un événement unique pour indiquer le changement d'action. Ainsi, par exemple, lorsque le seuil limite de 10 est atteint, que le système arrête de générer des événements et que l'action passe de Générer des événements à Déposer et générer des événements sur le 14e paquet, le système génère un onzième événement pour indiquer le changement d'action.

Exemple de détection et de seuil ou de suppression basée sur le débit pour l'ensemble de la politique

L'exemple suivant montre un agresseur tentant une attaque par déni de service sur les hôtes de votre réseau. De nombreuses connexions simultanées aux hôtes à partir des mêmes sources déclenchent un paramètre de contrôle des connexions simultanées à l'échelle de la politique. Le paramètre génère des événements et abandonne le trafic malveillant lorsqu'il y a cinq connexions à partir d'une même source en 10 secondes. En outre, un seuil de limite globale limite le nombre d'événements qu'une règle ou un paramètre peut générer à 10 événements en 20 secondes.

Comme l'illustre le diagramme, le paramètre à l'échelle de la politique génère des événements pour les dix premiers paquets correspondants et abandonne le trafic. Après le dixième paquet, le seuil limite est atteint. Par conséquent, pour les autres paquets, aucun événement n'est généré, mais les paquets sont abandonnés.

Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Si le débit échantillonné est supérieur au débit seuil au cours de la période d'échantillonnage en cours ou précédente, l'action basée sur le débit consistant à générer des événements et à abandonner le trafic se poursuit. L'action basée sur le débit ne s'arrête qu'à la fin d'une période d'échantillonnage, au cours de laquelle la fréquence échantillonnée est inférieure à la fréquence de seuil.



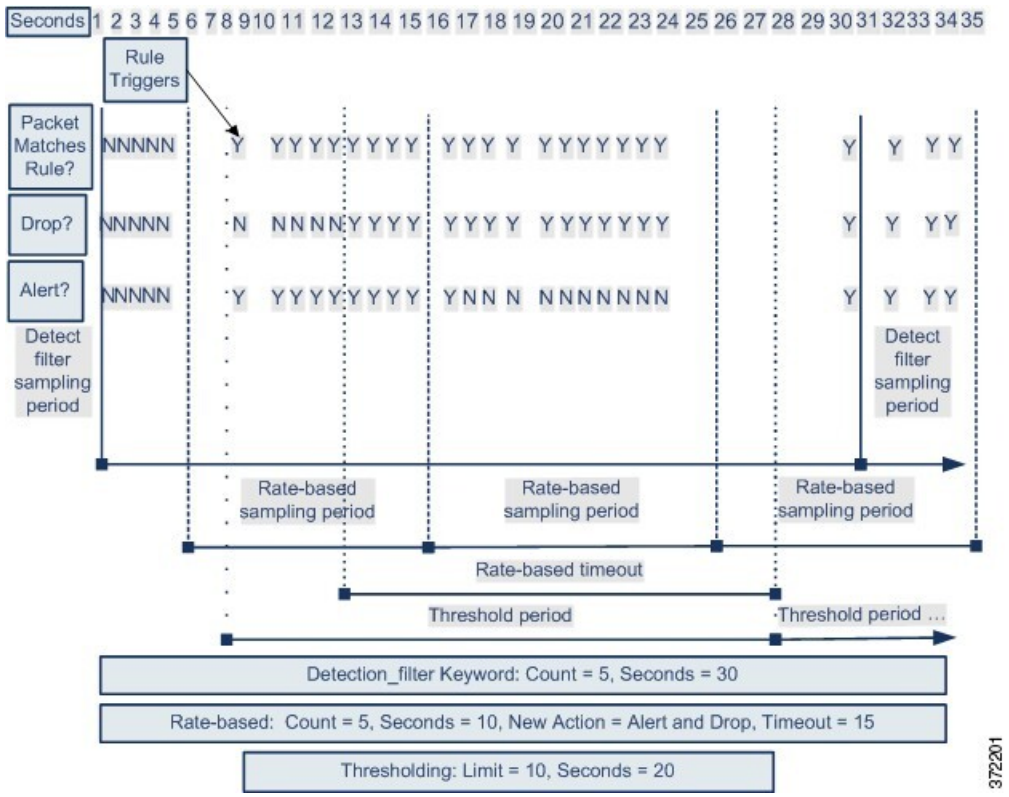
Notez que bien que cela ne soit pas illustré dans cet exemple, si une nouvelle action se déclenche en raison de critères basés sur le débit *après* l'atteinte d'un seuil, le système génère un événement unique pour indiquer le changement d'action. Ainsi, par exemple, si le seuil limite de 10 a été atteint, que le système arrête de générer des événements et que l'action passe aux événements Drop (Abandonner) et Generate (générer les événements) sur le 14e paquet, le système génère un onzième événement pour indiquer le changement d'action.

Exemple de détection basée sur le débit avec plusieurs méthodes de filtrage

L'exemple suivant montre un attaquant qui tente une connexion par force brute et décrit un cas dans lequel un mot-clé `detection_filter`, le filtrage basé sur le débit et le seuillage interagissent. Les tentatives répétées pour trouver un mot de passe déclenchent une règle qui inclut le mot-clé `detection_filter`, avec un nombre fixé à 5. Cette règle comporte également des paramètres de prévention des attaques basés sur le débit qui modifient l'attribut de règle pour Abandonner et générer des événements pendant 30 secondes lorsqu'il y a cinq résultats de règles en 15 secondes. En outre, un seuil limite la règle à 10 événements en 30 secondes.

Comme le montre le diagramme, les cinq premiers paquets correspondant à la règle n'entraînent pas de notification d'événement, car la règle ne se déclenche pas tant que le débit indiqué dans le mot-clé `detection_filter` n'est pas dépassé. Une fois la règle déclenchée, la notification d'événement commence, mais les critères basés sur le débit ne déclenchent la nouvelle action Abandon and Generate Events que lorsque cinq autres paquets se passent. Une fois que les critères basés sur le débit sont remplis, le système génère des événements pour les paquets 11 à 15 et abandonne les paquets. Après le quinzième paquet, le seuil limite est atteint. Par conséquent, pour les paquets restants, le système ne génère pas d'événements, mais abandonne les paquets.

Après l'expiration du délai basé sur le débit, notez que les paquets sont toujours abandonnés dans la période d'échantillonnage basé sur le débit qui suit. Comme la fréquence échantillonnée est supérieure à la fréquence seuil de la période d'échantillonnage précédente, la nouvelle action se poursuit.



Options et configuration de prévention contre les attaques basées sur le débit

La prévention des attaques basée sur le débit détecte les schémas de trafic anormaux et tente de minimiser l'impact de ce trafic sur les demandes légitimes. Les attaques basées sur le débit présentent généralement l'une des caractéristiques suivantes :

- Tout trafic contenant un trop grand nombre de connexions incomplètes aux hôtes sur le réseau, indiquant une attaque par inondation SYN
- Tout trafic contenant un nombre excessif de connexions complètes aux hôtes sur le réseau, indiquant une attaque par inondation de connexion TCP/IP
- Correspondances excessives de règles dans le trafic vers une ou des adresses IP de destination en particulier ou provenant d'une ou d'adresses IP source en particulier
- Un nombre excessif de correspondances pour une règle particulière pour l'ensemble du trafic

Dans une politique d'analyse de réseau, vous pouvez configurer la détection de flux SYN ou TCP/IP pour l'ensemble de la politique; Dans une politique de prévention des intrusions, vous pouvez définir des filtres basés sur le débit pour des règles de prévention des intrusions ou de préprocesseur individuelles. Notez que vous ne pouvez pas ajouter manuellement un filtre basé sur le débit aux règles GID 135 ni modifier l'état de leurs règles. Les règles portant le GID 135 utilisent le client comme valeur source et le serveur comme valeur de destination.

Lorsque **la prévention des attaques SYN** est activée, la règle 135:1 se déclenche si une condition de fréquence définie est dépassée.

Lorsque **le contrôle des connexions simultanées** est activé, la règle 135:2 se déclenche si une condition de débit définie est dépassée, et la règle 135:3 se déclenche si une session se ferme ou expire.

Remarque L'inspection d'équilibre de charge des périphériques entre les ressources internes. Lorsque vous configurez la prévention des attaques basée sur le débit, vous configurez le débit de déclenchement par ressource, et non par périphérique. Si la prévention des attaques basée sur le débit ne fonctionne pas comme prévu, vous devrez peut-être réduire le débit de déclenchement. Il déclenche une alerte si les utilisateurs envoient trop de tentatives de connexion dans des intervalles de temps prescrits. Par conséquent, il est recommandé de limiter le débit à la règle. Pour obtenir de l'aide sur la détermination du débit approprié, communiquez avec le service d'assistance.

Chaque filtre basé sur le débit contient plusieurs composants :

- Pour les paramètres de source ou de destination à l'échelle de la politique ou basés sur des règles, la désignation de l'adresse réseau
- Le taux de correspondance de règles, que vous configurez comme nombre de correspondances de règles dans un nombre spécifique de secondes
- Une nouvelle action à entreprendre lorsque le débit est dépassé

  Lorsque vous définissez un paramètre basé sur le débit pour l'ensemble de la politique, le système génère des événements lorsqu'il détecte une attaque basée sur le débit et peut abandonner le trafic lors d'un déploiement en ligne. Lorsque vous définissez des actions basées sur le débit pour des règles individuelles, trois actions sont disponibles : Générer des événements, Supprimer et générer des événements, et Désactiver.
- La durée de l'action, que vous configurez comme valeur de délai d'expiration

Notez qu'une fois démarrée, la nouvelle action se produit jusqu'à ce que le délai soit atteint, même si le débit tombe en dessous du débit configuré pendant cette période. À l'expiration du délai, si le débit est descendu sous le seuil, l'action de la règle revient à l'action initialement configurée pour la règle. Pour les paramètres à l'échelle de la politique, l'action revient à l'action de chaque règle correspond au trafic ou s'arrête s'il ne correspond à aucune règle.

Vous pouvez configurer la prévention des attaques basée sur le débit dans un déploiement en ligne pour bloquer les attaques, de façon temporaire ou permanente. Sans configuration basée sur le débit, les règles définies sur Générer des événements créent des événements, mais le système ne supprime pas de paquets pour ces règles. Cependant, si le trafic d'attaque correspond aux règles qui ont des critères basés sur le débit configurés, l'action de débit peut entraîner l'abandon de paquets pendant la période pendant laquelle l'action de débit est active, même si ces règles ne sont pas initialement définies sur Abandon et Generate Events .

Remarque Les actions basées sur le débit ne peuvent pas activer les règles désactivées ni abandonner le trafic correspondant aux règles désactivées. Cependant, si vous définissez un filtre basé sur le débit au niveau de la politique, vous pouvez générer des événements sur ou sur et abandonner le trafic qui contient un nombre excessif de paquets SYN ou d'interactions SYN/ACK au cours d'une période désignée.

Vous pouvez définir plusieurs filtres basés sur le débit sur la même règle. Le premier filtre répertorié dans la politique de prévention des intrusions a la priorité la plus élevée. À noter que lorsque deux actions de filtres basés sur le débit entrent en conflit, le système met en œuvre l'action du premier filtre basé sur le débit. De

même, les filtres basés sur le débit à l'échelle de la politique remplacent les filtres basés sur le débit définis sur les règles individuelles en cas de conflit entre les filtres.

Sujets connexes

Définition d'un état de règle dynamique à partir de la page Rules (Règles)

Prévention des attaques basée sur le débit, filtrage des détections et seuil ou suppression

Le mot-clé `detection_filter` empêche une règle de se déclencher jusqu'à ce qu'un nombre seuil de correspondances de règles se produise dans un temps spécifié. Lorsqu'une règle comprend le mot-clé `detection_filter`, le système suit le nombre de paquets entrants correspondant au modèle de la règle par période d'expiration. Le système peut compter les résultats pour cette règle à partir d'adresses IP source ou de destination particulières. Une fois que le débit dépasse le débit indiqué dans la règle, la notification d'événement pour cette règle commence.

Vous pouvez utiliser la fixation de seuils et la suppression pour réduire le nombre d'événements excessifs en réduisant le nombre de notifications d'événements pour une règle, une source ou une destination, ou en supprimant complètement les notifications pour cette règle. Vous pouvez également configurer un seuil de règle global qui s'applique à chaque règle qui n'a pas de seuil spécifique de remplacement.

Si vous appliquez la suppression à une règle, le système supprime les notifications d'événements pour cette règle pour toutes les adresses IP applicables, même si une modification d'action basée sur le débit se produit en raison d'un paramètre basé sur le débit propre à la politique ou propre à une règle.

Sujets connexes

Seuils de incidents d'intrusion
Configuration de la suppression des politiques de prévention des intrusions
Principes de base des seuils de règle globale

Configuration de la prévention des attaques basées sur le débit

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous pouvez configurer la prévention des attaques basée sur le débit au niveau de la politique pour arrêter les attaques par inondation SYN. Vous pouvez également arrêter un nombre excessif de connexions à partir d'une source ou vers une destination donnée.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (Paramètres).

Étape 5 Si **prévention des attaques basée sur le débit** sous **Détection de menaces spécifiques** est désactivée, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à c^té de **Prévention des attaques basées sur le débit**

Étape 7 Vous avez deux choix :

- Pour éviter les connexions incomplètes destinées à inonder un hôte, cliquez sur **Add** (ajouter) sous **Prévention des attaques SYN**.
- Pour éviter un nombre excessif de connexions, cliquez sur **Add** (ajouter) sous **Control Simultaneous Connections** (Contrôle des connexions simultanées).

Étape 8 Précisez comment vous souhaitez suivre le trafic :

- Pour suivre tout le trafic provenant d'une source ou d'une plage de sources spécifique, choisissez **Source** dans la liste déroulante **Track By** (suivre par), puis saisissez une adresse IP ou un bloc d'adresses dans le champ **Network** (Réseau).
- Pour suivre tout le trafic vers une destination ou une plage de destinations données, choisissez **Destination** dans la liste déroulante **Track By** (suivi par), puis saisissez une adresse IP ou un bloc d'adresses dans le champ **Network** (Réseau).

Remarque

- Ne saisissez pas l'adresse IP 0.0.0.0/0 dans le champ Network pour surveiller tous les sous-réseaux ou les adresses IP. Le système ne prend pas en charge cette adresse IP (qui est généralement utilisée pour identifier tous les sous-réseaux ou adresses IP) pour la prévention des attaques par débit.
- Le système suit le trafic séparément pour chaque adresse IP incluse dans le champ **Network** (réseau). Le trafic provenant d'une adresse IP qui dépasse le débit configuré entraîne des événements générés uniquement pour cette adresse IP. Par exemple, vous pourriez définir le bloc d'adresse CIDR source `10.1.0.0/16` pour le paramètre réseau et configurer le système pour générer des événements lorsque dix connexions simultanées sont ouvertes. Si huit connexions sont ouvertes à partir de la version 10.1.4.21 et six à partir de la version 10.1.5.10, le système ne génère pas d'événements, car aucune des sources n'a le nombre déclencheur de connexions ouvertes. Cependant, si onze connexions simultanées sont ouvertes à partir de la version 10.1.4.21, le système génère des événements uniquement pour les connexions à partir de la version 10.1.4.21.

  Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Étape 9 Précisez la fréquence de déclenchement pour le paramètre de suivi de fréquence :

- Pour la configuration d'une attaque SYN, saisissez le nombre de paquets SYN par nombre de secondes dans les champs **Rate** (Fréquence).
- Pour la configuration de connexions simultanées, saisissez le nombre de connexions dans le champ **Nombre**.

L'inspection d'équilibre de charge des périphériques entre les ressources internes. Lorsque vous configurez la prévention des attaques basée sur le débit, vous configurez le débit de déclenchement par ressource, et non par périphérique. Si la prévention des attaques basée sur le débit ne fonctionne pas comme prévu, vous devrez peut-être réduire le débit de déclenchement. Il déclenche une alerte si les utilisateurs envoient trop de tentatives de connexion dans des intervalles de temps prescrits. Par conséquent, il est recommandé de limiter le débit à la règle. Pour obtenir de l'aide sur la détermination du débit approprié, communiquez avec le service d'assistance.

Étape 10 Pour abandonner les paquets correspondant aux paramètres de prévention des attaques basées sur le débit, cochez la case **Drop** (Abandonner).

Étape 11 Dans le champ **Timeout** (délai d'expiration), saisissez le délai après lequel cesser de générer des événements (et, le cas échéant, des abandons) pour le trafic ayant le modèle correspondant de SYN ou de connexions simultanées.

Mise en garde La définition d'une valeur de délai d'expiration élevée peut bloquer complètement la connexion à un hôte dans un déploiement en ligne.

Étape 12 Cliquez sur **OK**.

Étape 13 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.